

**United States District Court**  
for the  
Western District of New York

**In the Matter of the Search of**

*(Briefly describe the property to be searched or identify the person by name and address.)*

INFORMATION ASSOCIATED WITH ACCOUNTS  
kewldad212@gmail.com and 646-470-0655, STORED AT  
PREMISES CONTROLLED BY GOOGLE, INC.

**Case No. 18-MJ-1040**

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Accounts kewldad212@gmail.com and 646-470-0655, stored at premises controlled by Google, Inc.,

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, Items to Be Searched for and Seized.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18, United States Code, Sections 1343, 1030(a)(4), and 1030 (a)(5)(C).

The application is based on these facts:

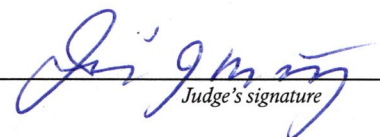
- ☒ continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

DAVID W. PEACOCK, JR.  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION  
Printed name and title

Sworn to before me and signed in my presence.

Date: January 30, 2018

  
Judge's signature

City and state: Buffalo, New York

JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE  
Printed name and Title

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     SS:  
CITY OF BUFFALO        )

I, David W. Peacock, Jr., being duly sworn, depose and state the following:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have served in this capacity for over nine years. I am currently assigned to the Cyber Squad, Buffalo Division, in Buffalo, New York and I have worked cyber matters, that is, matters focused on computer intrusions, throughout the entirety of my FBI career. I have experience in both criminal and national security investigations. Specifically, I have worked or assisted with matters involving unauthorized access to computer systems, counterintelligence, counterterrorism, Internet fraud, intellectual property rights, Innocent Images National Initiative, and theft of trade secrets. Prior to my employment in the FBI, I received a Bachelor's of Science in Computer Science. My work in the FBI, as well as training I received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. I have also conferred with other FBI Special Agents who have expertise and experience in cyber investigations and digital evidence.

2. I make this affidavit in support of an application for a search warrant authorizing the search of an email accounts controlled by the Internet Service Provider known as Google, Inc., 1600 Ampitheatre Parkway, Mountain View, California 94043.

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts.

4. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme) and Title 18 U.S.C. 1030(a)(4) (Fraud and related activity in relation to computers) and/or Title 18 U.S.C. 1030 (a)(5)(C) (Intentional access to a protected computer causing damage or loss) will be found in the accounts:

**kewldad212@gmail.com**  
**646-470-0655 (Google Voice)**

5. The account above is connected with accounts that were used in connection with the wire fraud scheme. The subject(s) have been found to use numerous email, phone number, and voice over internet protocol (VOIP) phone number (e.g., Google Voice)



accounts for varying periods of time in a likely effort to obfuscate the subject(s)'s identity. The use of multiple names and payment devices has left the true identity of the subject(s) undetermined. As with other accounts previously targeted in this investigation, **kewldad212@gmail.com** and **646-470-0655 (Google Voice)** likely contain evidence of schemes to defraud. More importantly, they could contain information, when viewed in context of other data obtained in the course of the investigation, that would identify the subject (or subjects) and possibly be used to provide a current location.

6. In my training and experience, I have learned that Google is a company that provides Internet electronic mail (email) access to the public, and that stored electronic communications, including opened and unopened email for subscribers, may be located on the computers owned or leased by these companies. Further, I am aware that computers located at Google contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein and further described in Attachments A and B.

7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.



**II. PROBABLE CAUSE JP MORGAN CHASE ACCOUNT 908201028 WAS USED TO COMMIT FRAUD AND SPECIFIED COMMUNICATION ACCOUNTS CONTAIN INFORMATION REGARDING THAT FRAUD**

8. On January 13, 2017, SCOTT DAVID LEUTHE contacted the FBI to report the loss of approximately \$150,000.00. Around the end of December 2016, \$49,000.00 was transferred from his Invesco Investment Service, Inc. ("Invesco") retirement account followed by a transfer of \$100,000.00 from the same account for a total of \$149,000.00. Prior to this event, on or about December 23, 2016, LEUTHE received a delivery from LegalZoom containing documents pertaining to the opening of a company, SDL Remodeling, LLC, in his name. LEUTHE had not requested the opening of this company. LEUTHE also learned a hold had been placed on his mail between on or about December 29, 2016 and December 31, 2016. He learned of the mail-hold when his mail was accidentally delivered and he received mail alerting him to the transfer of money from his Invesco retirement account.

9. A subpoena response from Invesco for LEUTHE's 401(k) account, identified by the plan name "Scott D Leuthe" and account number 77304, revealed the information in the paragraphs that follow.

10. On December 22, 2016, a loan request form was submitted in the amount of \$49,000.00. The money was to be deposited in JP Morgan Chase Bank account number 908201028. The title on that bank account was "SDL REMODELING LLC." The business address listed for SDL Remodeling, LLC was LEUTHE's home address: 510 Seneca Creek Rd, West Seneca, NY. The branch of the JP Morgan Chase Bank account was "Arthur Godfrey-141910." A form associated with the loan appeared to be signed "S Leuthe." The

response from Invesco also included LEUTHE's account application. A document from April 7, 2010, appeared to be signed "Scott D. Leuthe." This signature was clearly different than the signature observed as part of the December 22, 2016 loan application.

11. The Invesco response included correspondence sent to LEUTHE in regard to the \$49,000.00 loan which was dated December 27, 2016. This correlated with the time at which LEUTHE reported becoming alerted to the fraudulent loan.

12. The Invesco response also included a 401(k) distribution form for a one-time distribution in the amount of \$100,000.00. It was dated December 29, 2016. The distribution form appeared to be signed "S Leuthe," similar to the loan application. The dollar amounts reported the loan application and the distribution form added up to \$149,000.00 as reported by LEUTHE.

13. Prior to reporting the incident to the FBI, LEUTHE reported it to the West Seneca Police Department. The West Seneca Police Department provided the FBI with records pertaining to the fraudulent transfer of money from LEUTHE's Invesco account. Included among the records provided to the FBI were records obtained from JP Morgan Chase for account 908201028, the account which, as described above, was to receive the money transferred from LEUTHE's Invesco account. JP Morgan Chase records indicated account 90801028 was opened on December 16, 2016. The account title was "SDL REMODELING LLC." This was the same as the company opened in the name of LEUTHE as indicated in the package he had received from LegalZoom. JP Morgan Chase Bank

account 908201028 had a business address of 510 Seneca Creek Rd, West Seneca, NY, the home address of LEUTHE (the victim). A business signature card was issued upon opening of this account at the JP Morgan Chase Bank branch Arthur Godfrey-141910.

14. Open source research on the Internet revealed the address 474 W 41st Street, Miami Beach, Florida appears to be the address of the Arthur Godfrey branch of JP Morgan Chase Bank. This address appeared in the JP Morgan Chase Bank response as the location of an ATM withdrawal in the amount of \$15.00 on December 19, 2016. This was the same day the bank account 908201028 was opened. The person who opened the account was likely physically in Miami Beach, Florida.

15. The JP Morgan Chase Bank account 908201028 records showed a deposit of \$49,000.00 via The Bank of New York Mellon on behalf of "Scott D Leuthe West Seneca NY" on December 23, 2016. The "Order Bank" for that transfer was listed as "INVESCO INVESTMENT SERVICE, INC."

16. West Seneca Police Department provided records obtained from LegalZoom pertaining to the company SDL Remodeling, LLC as well. According to LegalZoom records, the order to create company SDL Remodeling, LLC was initiated on December 14, 2016. The name used was "Scott Leuthe" and the address used was LEUTHE's (the victim): 510 Seneca Creek Rd, West Seneca, NY.



**A. Accounts Not Targeted Herein But Provided for Background**

**manager@kewldad.com**

17. According to records obtained from LegalZoom, the email address manager@kewldad.com was a contact email address associated with the creation of the company SDL Remodeling, LLC. As explained above, SDL Remodeling, LLC was fraudulently created in the name of SCOTT DAVID LEUTHE (the victim) and subsequently used to open up JP Morgan Chase Bank account 908201028. That account was then used to fraudulently receive funds from LEUTHE's investment 401(k) account.

18. Records from Google in response to a subpoena confirmed manager@kewldad.com was an email registered through Google.

**kewldad.com**

19. The domain kewldad.com was identified as the domain of the email address manager@kewldad.com, which was used as the contact email address for the creation of SDL Remodeling, LLC according to LegalZoom record as described above.

20. Records from Google in response to a subpoena confirmed the domain kewldad.com was registered through Google. Services associated with the account included calendar, contacts, drive and docs [documents], Gmail, Google hangouts, Google+, groups for business, keep [used for notes and to-dos], and sites.

**kirkgerman382@gmail.com**

21. The email address kirkgerman382@gmail.com was the alternate email address provided for the account associated with kewldad.com according to records provided by Google in response to a subpoena. The email address manager@kewldad.com associated with domain kewldad.com was used as the contact email address with LegalZoom to fraudulently create the company SDL Remodeling, LLC in the name of SCOTT DAVID LEUTHE (the victim) as part of the scheme to transfer money from LEUTHE's 401(k) investment account.

**schoolboy117@gmail.com**

22. The email address schoolboy117@gmail.com was associated with the account for Google Voice number 804-220-0077 according to records provided by Google in response to a subpoena. Google Voice number 804-220-0077 was used as a contact phone number with JP Morgan Chase Bank for account 908201028. This was the bank account to which money from SCOTT DAVID LEUTHE's (the victim) 401(k) investment account was fraudulently transferred.

23. Results received pursuant to two court authorized search warrants, one for Google accounts manager@kewldad.com, kewldad.com, kirkgerman382@gmail.com, kyle.d.anderson05@gmail.com, and schoolboy117@gmail.com and a second for Google Voice accounts 804-220-0073, 804-220-0077, and 804-220-0078, signed by United States Magistrate Judge Michael J. Roemer on July 26, 2017 and subsequent investigation and analysis revealed the information in the proceeding paragraphs.

24. The email accounts kirkgerman382@gmail.com and schoolboy117@gmail.com shared common IP address logins. Given kirkgerman382@gmail.com was already connected with email account manager@kewldad.com because it was listed as the alternate email address for kewldad.com, it is highly likely the user of all three email accounts, kirkgerman382@gmail.com, manager@kewldad.com, and schoolboy117@gmail.com is the same person.

25. There were multiple emails in the kirkgerman382@gmail.com, manager@kewldad.com, and schoolboy117@gmail.com e-mail accounts addressed to different names which included gift card notices, invoices, credit and loan applications, and FedEx tracking updates which would seem to indicate additional fraudulent activity.

26. A voicemail for Google Voice account 804-220-0077 (associated with the JP Morgan Chase Account 908201028 and email account schoolboy117@gmail.com) was left by LegalZoom in regard to an order. This would have been prior to the fraud documented herein and likely indicates a pattern of fraud predating the incident first being investigated.

27. On July 6, 2017, schoolboy117@gmail.com sent an email to leewash54@yahoo.com containing personal identifying information for two individuals. The information included names, addresses, credit card numbers, social security numbers, and dates of birth. Such information could be used to carry out additional fraudulent transactions.



28. Uber invoices found in the emails of kirkgerman382@gmail.com and addressed to "Jordan" revealed the user took a flight from LaGuardia Airport in New York City to Miami International Airport on May 14, 2017. The fraudulent JPMorgan Chase Bank account was in the Miami Beach area.

**Phone Number 718-755-0761**

29. Emails produced by Google pursuant to a court authorized search warrant for accounts which included kirkgerman382@gmail.com and schoolboy117@gmail.com revealed these two accounts were also connected by a common phone number: 718-755-0761. Each email account received an email on February 2, 2017 referencing the phone number 718-755-0761, further supporting that these accounts are used by the same user(s). The email to kirkgerman382@gmail.com at 8:58 PM (EST) read as follows:

*Dear Kirk German,*

*Please note that the forwarding number (718) 755-0761 was deleted from your Google Voice account (kirkgerman382@gmail.com) because it was claimed and verified by another Google Voice user.*

*If you still want this forwarding number on your account and believe this was an error, please [click here](#) to learn more.*

*Thanks,*

*The Google Voice Team*

30. Similarly, the email to [schoolboy117@gmail.com](mailto:schoolboy117@gmail.com), sent the same day at 9:17 PM (EST) read as follows:

*Dear robert james,*

*Please note that the forwarding number (718) 755-0761 was deleted from your Google Voice account ([schoolboy117@gmail.com](mailto:schoolboy117@gmail.com)) because it was claimed and verified by another Google Voice user.*

*If you still want this forwarding number on your account and believe this was an error, please [click here](#) to learn more.*

*Thanks,*

*The Google Voice Team*

31. The same phone number, 718-755-0761, appeared in the records from LegalZoom associated with the creation of a company, DMann Electrical Contracting, LLC, in September 2016. DMann Electrical Contracting, LLC was a LegalZoom created company that had the same contact number, 804-220-0077, as SDL Remodeling, LLC. The contact names used in the creation of the DMann Electrical Contracting, LLC company were “Barry Seidel” and “Daniel Mannix.”

32. Notably, during the course of a search of a number of e-mail accounts conducted pursuant to a court authorized search warrant, there were emails to [schoolboy117@gmail.com](mailto:schoolboy117@gmail.com) addressed to “Barry Seidel.” One such email was from FedEx, sent October 16, 2016, notifying “Barry Seidel” of the suspension of a FedEx account.

**kewldad22@mail.com**

33. A search of the kirkgerman382@gmail.com account, conducted pursuant to a court authorized search warrant, revealed emails from Lyft, an online service used to request transportation, usually via a mobile device. One email, sent January 3, 2017, indicated the user was transported from “337 Terminal Dr” [Fort Lauderdale, Florida] to “124 71<sup>st</sup> St, Miami Beach.” Notably, the JPMorgan Chase Bank account used to defraud victim SCOTT DAVID LEUTHE was opened in Miami Beach, Florida. Records provided by Lyft pursuant to a subpoena, revealed an account with the contact number 718-755-0761. As previously mentioned, 718-755-0761 was associated with the schooboy117@gmail.com and kirkgerman382@gmail.com. That Lyft account had the contact email address kewldad22@mail.com.

34. Further, records obtained via subpoena from 1&1 Mail & Media for kewldad22@mail.com associated this account with the name “Barry Seidel.” As mentioned earlier, “Barry Seidel” appeared in LegalZoom records for companies DMann Electrical Contracting, LLC and BarrySdel Electrical Contracting, LLC, both using the contact number 804-220-0077 (a phone number used as part of the scheme to defraud victim SCOTT DAVID LEUTHE). The name “Barry Seidel” also appeared in emails to schoolboy117@gmail.com as described above.

35. Therefore, it is likely kewldad22@mail.com is used by the same subject(s) of this investigation.



**yanks4ever3@mail.com**

36. The email address yank4ever3@mail.com, according to records from LegalZoom, was the listed contact e-mail address for the creation of company PeteWay Roofing, LLC. The contact number for PeteWay Roofing, LLC was 804-220-0077, the same Google Voice number used as a contact phone number with JP Morgan Chase Bank for account 908201028, which was the bank account to which money from LEUTHE's 401(k) investment account was fraudulently transferred.

37. Additionally, the LegalZoom account for BarrySdel Electrical Contracting, LLC (associated with email address fishermanstatus@aol.com and name "Barry Seidel") shared a common login with the LegalZoom account for PeteWay Roofing, LLC (associated with yanks4ever3@mail.com). These particular accesses to the accounts occurred on September 26, 2016 using IP address 167.160.113.14. The accesses were within 10 minutes of each other, likely indicating it was the same user.

38. Records obtained from Google pursuant to a court authorized search warrant, which included email account kirkgerman382@gmail.com, revealed fishermanstatus@aol.com was the recovery email address for the kirkgerman382@gmail.com account.

39. The email account kewldad22@mail.com also shared a common login with email account yanks4ever3@mail.com. Both used IP address 166.149.39.51 on March 26, 2017 and March 27, 2017.

40. Therefore, it is likely yanks4ever3@mail.com is used by the same subject(s) of this investigation.

**C. Targeted Account: 646-470-0655 (Google Voice)**

41. Google Voice number **646-470-0655** was found to be associated with email account kirkgerman382@gmail.com. Emails obtained pursuant to a search warrant for accounts including kirkgerman382@gmail.com contained emails with invoices from Uber, an application used to request transportation, usually from mobile device such as a cell phone. The invoices, addressed to "Jordan," revealed the user took a flight from LaGuardia Airport in New York City to Miami International Airport on May 14, 2017. The fraudulent JPMorgan Chase Bank account was in the Miami Beach area. Subpoenaed records from Uber revealed an account under the name "Jordan Clarkson" with email address kirkgerman382@gmail.com and phone number **646-470-0655**.

42. The email account kewldad212@gmail.com was the registered email account for Google Voice phone number **646-470-0655**. This was determined from records provided by Google, Inc. in response to a subpoena.

43. Furthermore, it should be noted because kewldad212@gmail.com was the registered email account for **646-470-0655**, The SMS texting number registered for kewldad212@gmail.com, as identified in records provided by Google, Inc. pursuant to a subpoena, was 804-220-0077, the same Google Voice number used as a contact phone number with JP Morgan Chase Bank for account 908201028, which was the bank account to which

money from LEUTHE's 401(k) investment account was fraudulently transferred. Therefore, it is likely Google Voice number **646-470-0655**, **kewldad212@gmail.com**, and Google Voice number 804-220-0077 were all used by the same subject(s) of investigation.

**D. Targeted Account: kewldad212@gmail.com**

44. The targeted email account **kewldad212@gmail.com** was found to be connected with other communication accounts associated with the subject(s) of investigation. The subject(s) have been found to use numerous email, phone number, and voice over internet protocol (VOIP) phone number (e.g., Google Voice) accounts for varying periods of time in a likely effort to obfuscate the subject(s)'s identity. As with other accounts previously targeted in this investigation, **kewldad212@gmail.com** likely contains evidence of schemes to defraud. More importantly, it could contain information, when viewed in context of other data obtained in the course of the investigation that would identify the subject (or subjects) and possibly be used to provide a current location.

45. The email account **kewldad212@gmail.com** was the registered email account for Google Voice phone number **646-470-0655**. This was determined from records provided by Google, Inc. in response to a subpoena. That number and its registered email address **kewldad212@gmail.com** are believed to be used by the same subject(s) of investigation for the following reasons:

- The Uber ride on May 14, 2017 dropped the individual off in the vicinity of 6475-6477 Collins Avenue, Miami Beach, Florida. Accounts **kewldad22@mail.com** and **yanks4ever3@mail.com**, accounts believed to be used by subject(s) of investigation as



described earlier in this affidavit, both were accessed from IP address 216.189.188.131. The access for kewldad22@mail.com occurred on March 24, 2017 and the access for yanks4ever3@mail.com occurred on April 5, 2017. Subpoenaed records from Atlantic Broadband indicated the IP address 216.189.188.131 was leased between February 7, 2017 and July 3, 2017 to the apartment 703 at address 6450 Collins Avenue, Miami Beach, Florida. Mapped out, this location is across the street from the drop-off location of the May 14<sup>th</sup> Uber ride.

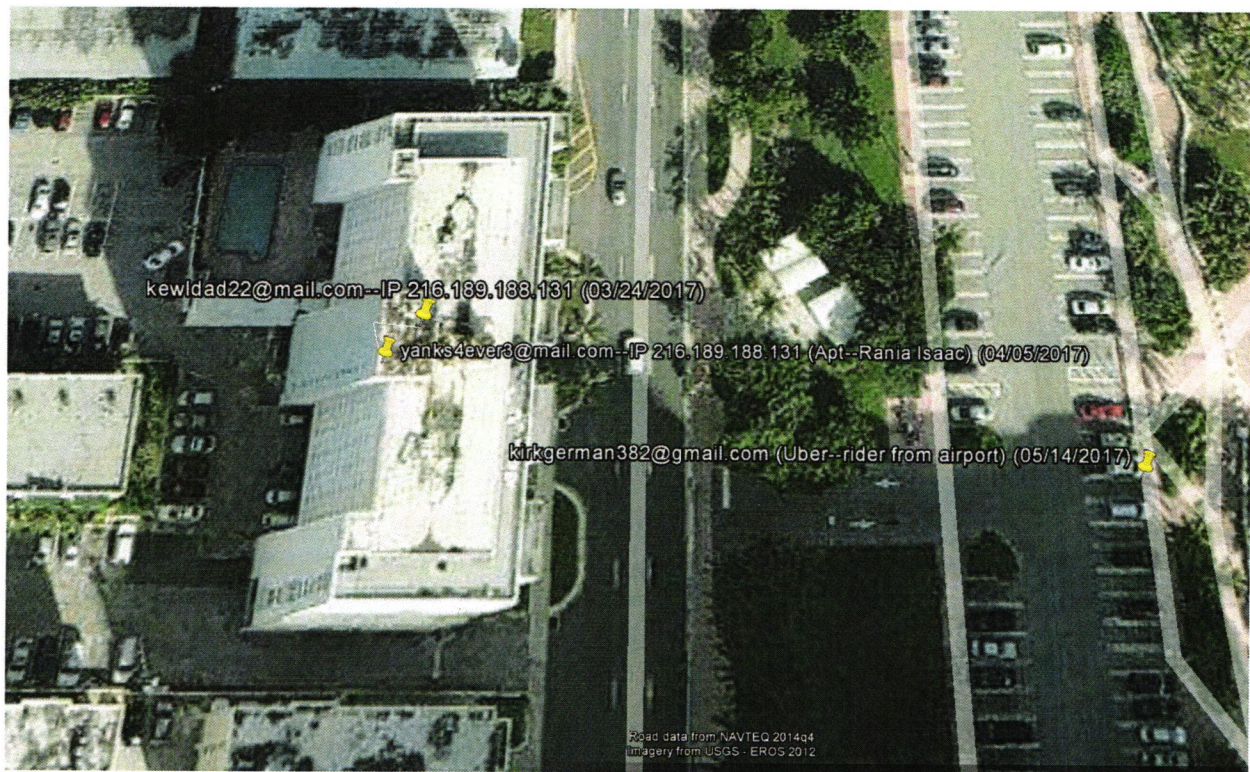


Figure 1

- The SMS texting number registered for kewldad212@gmail.com, as identified in records provided by Google, Inc. pursuant to a subpoena, was 804-220-0077, , the same Google

Voice number used as a contact phone number with JP Morgan Chase Bank for account 908201028, which was the bank account to which money from LEUTHE's 401(k) investment account was fraudulently transferred.

46. The subpoenaed records provided by Google, Inc. for kewldad212@gmail.com indicated among the enabled services for the account were "Android" and "Location History." Content account, as opposed to some previously observed in the investigation, may be more likely to provide information as to the location of the subject which may lead to a true identity.

47. In summary, given the aforementioned facts, I submit there is probable cause that a person (or persons) acquired information identifying victim SCOTT DAVID LEUTHE and his Invesco retirement account. On December 14, 2016, LEUTHE's (the victim) information was used to open company SDL Remodeling, LLC via services provided by LegalZoom. It should be noted, the name SDL Remodeling, LLC includes LEUTHE's initials "SDL." On December 19, 2016, the company SDL Remodeling, LLC was used to open a bank account (908201028) with JP Morgan Chase Bank in Miami Beach, Florida. On December 23, 2016, a loan application was place with Invesco to move LEUTHE's (the victim) money, \$49,000.00, to the JP Morgan Chase Bank account 908201028. A distribution request was filed with Invesco on December 29, 2016 to move an additional \$100,000.00 of LEUTHE's money to the JP Morgan Chase Bank account 908201028. The use of SDL Remodeling, LLC to open the bank account was likely for the purpose of making the transactions appear to be authorized by the victim, LEUTHE, without him being alerted. The



fact that LEUTHE reported a hold was placed on his mail further supports the person (or persons) devising the scheme to defraud was taking steps to avoid having LEUTHE alerted.

48. Contact information used to create accounts in furtherance of the scheme to transfer money from the victim's 401(k) investment account has led to the identification of additional communication accounts which have contained information likely pertaining to fraud and about the subject that has yet to be identified. Accounts such as kirkgerman382@gmail.com and Google Voice number 804-220-0077 were identified early in the investigation as being associated with the scheme to defraud. Both are likely used by the same subject(s) and both are connected to the targeted accounts **kewldad212@gmail.com** and **646-470-0655** (Google Voice). The accounts **kewldad212@gmail.com** and **646-470-0655** (Google Voice) likely contain evidence of fraud, identity theft, and possibly information that could help locate and identify the subject(s) of the investigation. Additionally, analysis of cookies associated with these account could provide information regarding device and other accounts used by the subject(s) of investigation. Identifying current devices and accounts used by the subject(s) is important for locating and identifying the subject(s) who use multiples aliases and payment devices.

### **III. BACKGROUND REGARDING COMPUTER, THE INTERNET, AND EMAIL**

49. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage



facility or communications facility directly related to or operating in conjunction with such device.

50. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

51. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual

computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs's servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

52. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.

#### **IV. BACKGROUND REGARDING GOOGLE**

53. Based on my training and experience, I have learned the following about Google:

a. Google is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, city/zip code, and other personal/biographical information. However, Google does

not verify the information provided. As part of its services, Google also provides its subscribers with the ability to set up email accounts;

b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information. As part of its business records, Google logs cookies used by and associated with Google users. Google retains cookie data for 180 days based on user login activity. Google does not preserve this data;

c. Subscribers to Google may access their accounts on servers maintained or owned by Google from any computer connected to the Internet located anywhere in the world;

d. Any email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely;

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at Google, but that message will



remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;

f. A Google subscriber can store files, including emails and image files, on servers maintained and/or owned by Google; and

g. Emails and image files stored on a Google server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Google server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Google servers.

h. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation.

This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

#### **V. BACKGROUND REGARDING GOOGLE VOICE**

54. Google Voice is an internet-based communications service that allows users to control multiple phone lines or phone accounts through a single Google account. Anyone with a Google account may sign up for Google Voice. A single Google account can be used to access all of the online service offered by Google, such as Google Email, Google Checkout, or Google Talk. Google Voice advertises itself as a phone management system. A user is assigned a 10-digit US telephone number. Google Voice works with mobile phones, desk phones, work phones, and Voice Over Internet Protocol (VOIP) lines. Incoming phone calls to the Google Voice number will then ring simultaneously on all of the user's configured phones or to the account's Google Talk feature, which is an online video and voice chatting service similar to Skype.

55. A Google Voice account combines many traditional cell phone services with the features of an email or online storage account. For example, a user may receive voicemail at a Google Voice number, record calls, transcribe voicemails, and send text or instant messages. Google Voice offers the ability to send and receive text messages to an email address or cell phone, and then store that data online. Voicemail messages left at a Google Voice number can be converted to a text format and then emailed or texted to the user account.

56. Because a Google Voice account is associated with a general Google account, which has email capability, users have access to the traditional features of an email account. Unless the sender of the email specifically deletes the email or text, the message can remain in the system indefinitely.

## **VI. BACKGROUND REGARDING GOOGLE AND COOKIES**

57. According to representatives of Google, the company keeps records that can reveal Google accounts accessed from the same electronic device, such as the same computer or cellular phone, including account that are linked by “cookies,” which are small pieces of text sent to the user’s Internet browser when visiting websites.

58. A cookie is a small file maintained on a user’s computer which can store data for a specific web browser session, or the cookie can be persistent so that it may be used for future web browsing sessions. The cookie can maintain data such as user preferences.



59. The following information regarding cookies was found on the Internet at URL <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies> (Mozilla develops the Firefox web browser):

- a. An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol.
- b. Cookies are mainly used for three purposes:
  - i. Session management  
Logins, shopping carts, game scores, or anything else the server should remember.
  - ii. Personalization  
User preferences, themes, and other settings.
  - iii. Tracking  
Recording and analyzing user behavior

### **Creating Cookies**

60. When receiving an HTTP request, a server can send a Set-Cookie header with the response. The cookie is usually stored by the browser, and then the cookie is sent with requests made to the same server inside a Cookie HTTP header. An expiration date or duration can be specified, after which the cookie is no longer sent. Additionally, restrictions to a specific domain and path can be set, limiting where the cookie is sent.

**VII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

61. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**VIII. CONCLUSION**

62. Based on the foregoing, I believe there is probable cause to believe that the user(s) of **kewldad212@gmail.com** and **646-470-0655 (Google Voice)** has committed violations of 18 U.S.C. § 1343; having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme, and that evidence of that criminal violation, as specifically described in Attachment A to this application, is presently located in the subject(s)'s communications. There could also exist evidence of Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers, and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss) because unauthorized access to a computer is often used to acquire personal identifying information to carry out such schemes to defraud.

63. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe, and I do believe, that in the account **kewldad212@gmail.com** and **646-470-0655 (Google Voice)**, located on computer systems owned, maintained, and/or operated by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043, there exist evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme). I therefore respectfully request that the Court issue a search warrant directed to Google for (1) the email and Google Voice contents and other information described in Attachment A and following the search procedure described in Attachment B and (2) for all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, creation IP address, recovery email address, or telephone number, and the subscriber records, not content, for those newly identified accounts, following the search procedure described in Attachment B.

64. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

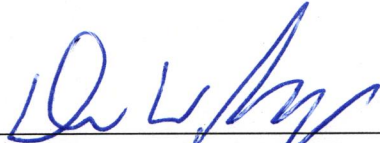
65. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



**IX. REQUEST FOR SEALING**

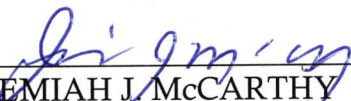
66. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal for 60 days or until further order of this Court.

DATED: Buffalo, New York, January 30, 2018.

  
\_\_\_\_\_  
DAVID W. PEACOCK, JR.  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed to before

me this 30th day of January, 2018.

  
\_\_\_\_\_  
JEREMIAH J. MCCARTHY  
United States Magistrate Judge

**ATTACHMENT A**  
**Property to be Searched**

This warrant applies to information associated with the following accounts stored at premises owned, maintained, controlled, or operated by Google, Inc., 1600 Ampitheatre Parkway, Mountain View, California 94043.

**kewldad212@gmail.com**  
**646-470-0655 (Google Voice)**

**ATTACHMENT B**

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Google, Inc. ("Google"), to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Google, personnel by law enforcement agents. Google, personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Google, system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;
5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.



**I. Information to be disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google, is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails stored in the account, including copies of emails sent from the account;
- b. The contents of communications to include, but not limited to voice calls, voice records, and text messages;
- c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment(including any creditor bank account number);
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- e. All content and subscriber information relating to Google Picasa, Google+, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, Google Hangouts, Google Photos, and Google Profile;
- f. Any and all Google accounts listed on the subscriber's Friends list;

g. All records pertaining to communications between Google, and any person regarding the account, including contacts with support services and records of actions taken.

h. All records pertaining to the location history of the account, to include GPS data, especially relating to Google and "Android" and "Location History" enabled services:

All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation precision measurement information such as timing advance or per call measurement data, Wi-Fi location, and/or Bluetooth location. Such data shall include the GPS coordinates, the dates and times of all location recordings, and origin of how the location recordings were obtained and estimated radius.

i. For all Google accounts that are linked to any of the accounts listed in Attachment A by cookies, creation IP address, recovery email address, or telephone number, provide:

All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration,

methods of connecting, log files, and means and source of payment(including any creditor bank account number);

## **II. Information to be searched for and seized by the government**

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme) and/or Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers, and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss) for each account or identifier listed on Attachment A, information pertaining to:

- a. The unauthorized access of email accounts;
- b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and their co-conspirators, the names, addresses, and locations of victims, and any disposition of the proceeds of the crimes under investigation, including,
- c. Records relating to who created, used, or communicated with the account or identifier
- d. For any and all accounts identified as being associated with targeted account through cookies, creation IP address, recovery email address, or telephone number,



all subscriber records or information, not including contents, of Records include, but are not limited to, records relating to who created, used, or communicated with the account or identifier